Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1-6 (Cancelled)

7. (Currently amended) A method of establishing communication between a first correspondent and a second correspondent, each of said correspondents having a respective identity, said first correspondent having a private key and a public key derived therefrom, said method comprising the steps of:

a) said second correspondent obtaining said public key of said first correspondent;

b) said second correspondent sending a short-lived public key and said second correspondent's identity to said first correspondent;

c) said first correspondent combining its private key with said short-lived public key and generating a pair of secret keys therefrom;

d) said first correspondent using a first of said pair of secret keys to compute a first MAC on its identity, said second correspondent's identity, a random challenge, and said short-lived public key;

e) said first correspondent sending its identity, said random challenge, and said first MAC to said second correspondent, thereby requesting registration;

f) said second correspondent using [[said]] a short-lived private key corresponding to said short-lived public key and said first correspondent's public key to generate said pair of secret keys;

g) said second correspondent verifying said first MAC using said first of said pair of secret keys;

h) said second correspondent using said first of said pair of secret keys to compute a second MAC on its identity, said first correspondent's identity, said random challenge, and said short-lived public key;

i) said second correspondent sending said MAC to said first correspondent, thereby registering said first correspondent;

j) said first correspondent verifying said second MAC using said first of said pair of secret keys;

k) said correspondents each computing a pair of session keys from a second of said pair of secret keys, said short-lived public key, and said random challenge; and

l) said correspondents using at least one of said session keys in a secure communication.

8. (Original) A method according to claim 7, said first correspondent being a mobile station and said second correspondent being a base station.

9. (Original) A method according to claim 8, said secure communication being a call originated by said mobile station.

10. (Original) A method according to claim 8, said secure communication being a call terminating at said mobile station.

11. (Original) A method according to claim 8, said secure communication being a data exchange between said stations.

12. (Original) A method according to claim 11, said data exchange being used for internet browsing.

13. (Original) A method according to claim 11, said data exchange being used for financial transactions.

14. (Original) A method according to claim 7, said second correspondent obtaining said public key from a service provider of said first correspondent.

15. (Original) A method according to claim 14, said service provider obtaining said public key by a manual exchange at a distributor outlet.

16. (Original) A method according to claim 15, said public key being transmitted to said service provider using a dial-up connection.

17. (Original) A method according to claim 14, said service provider obtaining said public key by an exchange at manufacture time.

18. (Original) A method according to claim 17, said exchange comprising the steps of a manufacturer retrieving said public key, and transmitting said public key to said service provider.

19. (Original) A method according to claim 14, said service provider obtaining said public key by an over-the-air exchange.

20. (Original) A method according to claim 19, said over-the-air exchange being secured using a password established between a user of said mobile station and said service provider.

21. (Original) A method according to claim 19, said over-the-air-exchange being secured using a password embedded in said mobile station at manufacture time.

22. (Original) A method according to claim 7, said second correspondent being a service provider of said first correspondent.

23. (Currently amended) A method according to claim 7, the [[two]] MACs computed in [[step (e)]] steps (d) and (h) each incorporating a value, said values being distinct from each other.

24. (Original) A method according to claim 8, wherein the value used in said mobile station MAC is 2 and said base station MAC is 3.

25. (Original) A method according to claim 7, said private keys, said public keys, and said MACs computed using elliptic curve cryptography.

26. (Original) A method according to claim 8, said elliptic curve having a cofactor t, said short-lived public key being bP, said mobile station private key being m, and said pair of secret keys being generated from a shared secret tmbP.

27. (Original) A base station for use in a communication system having at least one mobile station, each of said mobile stations having a secret key pair comprising a secret private key and a secret public key derived from said private key, access to said secret public key being restricted to a secure environment including said base station, said base station initiating communications with a respective one of said mobile stations by generating an ephemeral private key, obtaining therefrom a corresponding ephemeral public key, and forwarding said ephemeral public key to said mobile station, said base station computing

a shared secret to be shared with said one of said mobile stations from said ephemeral key pair and said secret key pair to permit authentication of said stations to one another.

28. (Original) A base station according to claim 27, wherein said base station obtains access to said secret public key from a service provider.

29. (Original) A base station according to claim 27, wherein said base station is a service provider of said mobile station.

30. (Original) A base station according to claim 29, wherein said base station obtains said public key by a manual exchange at a distributor outlet.

31. (Original) A base station according to claim 29, wherein said base station receives said public key using a dial-up connection.

32. (Original) A base station according to claim 29, wherein said base station obtains said public key by an exchange at manufacture time.

33. (Original) A base station according to claim 32, wherein said exchange comprises the manufacturer retrieving said public key, and transmitting said public key to said base station.

34. (Original) A base station according to claim 32, wherein said base station obtains said public key by an over-the-air exchange.

35. (Original) A base station according to claim 34, wherein said over-the-air exchange is secured using a password established between a user of said mobile station and said base station.

36. (Original) A base station according to claim 34, wherein said over-the-air-exchange is secured using a password embedded in said mobile station at manufacture time.

37. (Original) A base station according to claim 27, wherein said secret key pair, said ephemeral key pair, and said authentication use elliptic curve cryptography.

38. (Original) A method of establishing communications between a base station and a mobile station, wherein said mobile station has a secret key pair comprising a secret private key and a secret public key derived from said secret key, said method comprising the base station performing the steps of:

a) accessing said secret public key of said mobile station;

b) generating an ephemeral secret key;

c) obtaining from said ephemeral secret key a corresponding ephemeral public key;

d) forwarding said ephemeral public key bP to said mobile station; and

e) computing a shared secret from said ephemeral key pair and said secret key pair to permit authentication of said stations to one another.

39. (Original) A method according to claim 37, said base station accessing said secret public key by receiving said public key from a service provider.

40. (Original) A method according to claim 37, said base station being a service provider of said mobile station.

41. (Original) A method according to claim 39, said base station obtaining said public key by a .manual exchange at a distributor outlet.

42. (Original) A method according to claim 39, said base station receiving said public key using a dial-up connection.

43. (Original) A method according to claim 39, said base station obtaining said public key by an exchange at manufacture time.

44. (Original) A method according to claim 42, said exchange comprising the manufacturer retrieving said public key, and transmitting said public key to said base station.

45. (Original) A method according to claim 42, said base station obtaining said public key by an over-the-air exchange.

46. (Original) A method according to claim 44, said over-the-air exchange being secured using a password established between a user of said mobile station and said base station.

47. (Original) A method according to claim 44, said over-the-air-exchange being secured using a password embedded in said mobile station at manufacture tine.

48. (Original) A method for authenticating a first correspondent and a second correspondent in a communication system, wherein the first correspondent has a private key and public key pair, said method comprising the steps of:

a) said second correspondent transmitting a short term public key along with an identifier to said first correspondent;

b) said first correspondent combining its private key with the second correspondent's short term public key and generating a pair of shared secret keys;

c) the correspondents using the first of said pair of shared secret keys for mutual authentication between said first and second correspondent;

d) the correspondents using the second shared secret key of said pair of shared secret keys for establishing a secret session key;

e) the correspondents using said secret session key to provide confidentiality for authenticated communications in the communication system;

said mutual authentication characterised in that the first correspondent authenticates itself to the second correspondent using its private key, and the second correspondent authenticates itself to the first correspondent using the first correspondent's public key obtained by said second correspondent from a trusted correspondent.